ID: 510689
Sample Name:
SecuriteInfo.com.Variant.Razy.980776.8232.dll
Cookbook: default.jbs
Time: 05:09:04
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

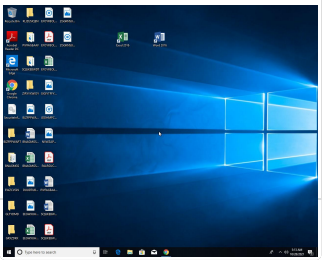
Windows Analysis Report SecuriteInfo.com.Variant.Raz…

Overview

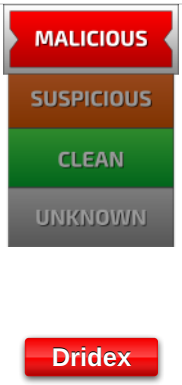
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.980776.8232.dll
Analysis ID:	510689
MD5:	6df0687582c592e.
SHA1:	53780def0699c05.
SHA256:	90877ec621cc53…
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

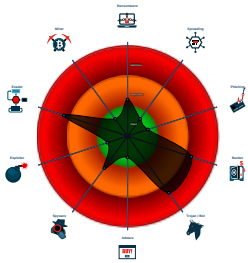


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Found detection on Joe Sandbox Clo…
- Detected Dridex e-Banking trojan
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Queries the installation date of Wind…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4248 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2248 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6340 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5016 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll,Bluewing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6332 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll,Earth MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6352 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll,Masterjust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 10444,
  "C2 list": [
    "192.46.210.220:443",
    "143.244.140.214:808",
    "45.77.0.96:6891",
    "185.56.219.47:8116"
  ],
  "RC4 keys": [
    "9fRysqcdPgZffBlroqJaZHyCvLvD6BUV",
    "syF7NqCylLS878kcIy9w5XeI8w6uMrqVwowz4h3uWHHlWsr5ELTiXic3wgqbllkcZyNGwPGihI"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.429863191.0000000003410000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000003.404224619.0000000004740000.00000040.00000010.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.690890687.000000006E9F1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.690396403.000000006E9F1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000003.420461174.0000000004120000.00000040.00000001.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.475db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.3.rundll32.exe.475db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.3.rundll32.exe.492db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
5.3.rundll32.exe.342db55.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.3.rundll32.exe.413db55.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

Detected Dridex e-Banking trojan

System Summary:

Found detection on Joe Sandbox Cloud Basic with higher score

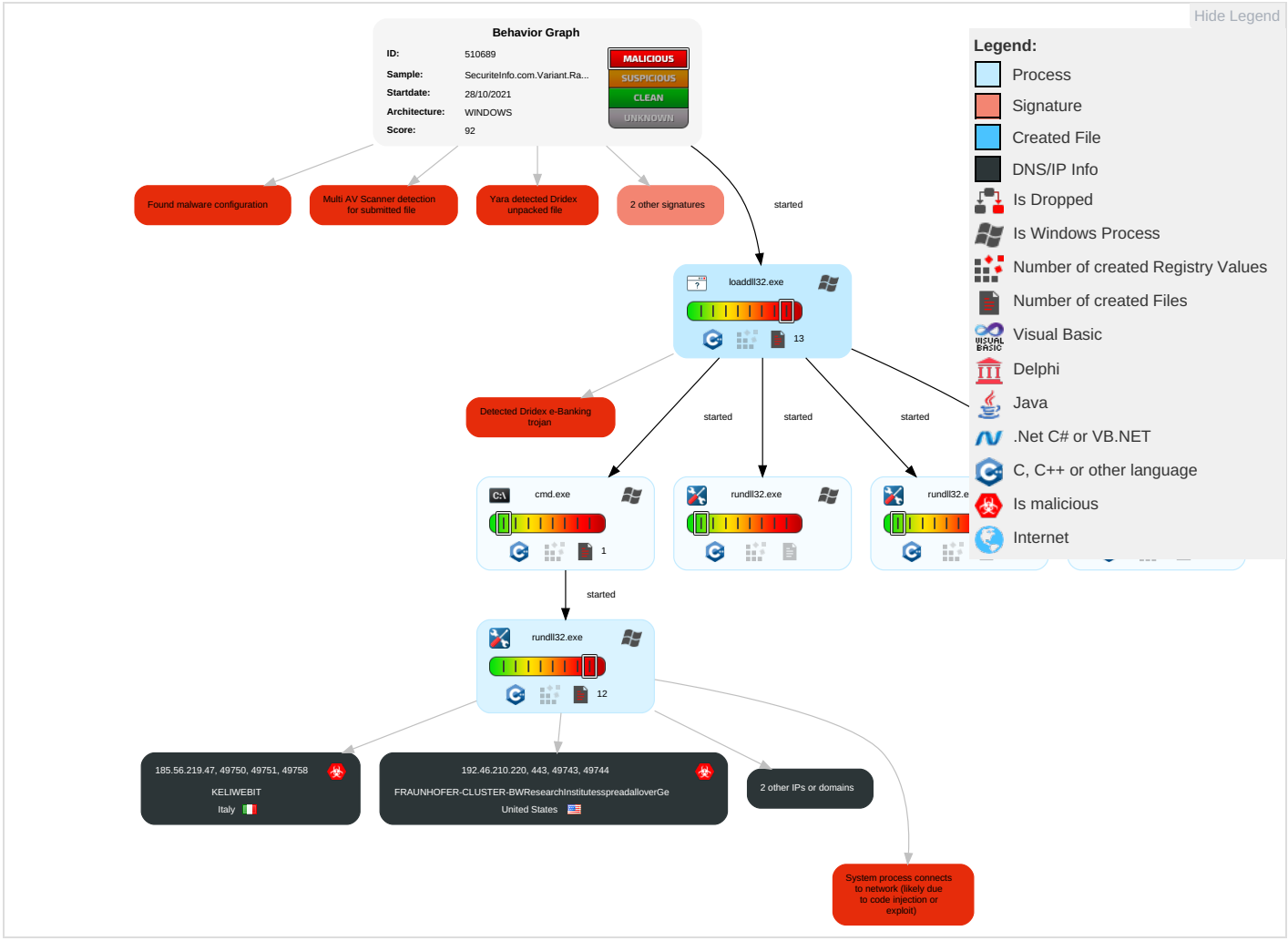
HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Process Injection 1 1 2	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Razy.980776.8232.dll	6%	Virustotal		Browse
SecuriteInfo.com.Variant.Razy.980776.8232.dll	18%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://143.244.140.214:808/hy	0%	URL Reputation	safe	
http://https://192.46.210.220/w	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/aenh.dll	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://185.56.219.47:8116/ion	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/	0%	URL Reputation	safe	
http://https://45192.46.210.220/	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/n	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/r	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/s	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/oft	0%	URL Reputation	safe	
http://https://192.46.210.220/#	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/m	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/fW	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/	0%	URL Reputation	safe	
http://https://192.46.210.220/7.0.96:6891/	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/soft	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/4	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/la	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/14	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/der	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/Q#	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/N	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/:	0%	Avira URL Cloud	safe	
http://https://143.244.140.214/	0%	URL Reputation	safe	
http://https://185.56.219.47/	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/F	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/A	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/q	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/I	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/dv	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/H	0%	Avira URL Cloud	safe	
http://https://143.244.140.214:808/l	0%	URL Reputation	safe	
http://https://192.46.210.220/S	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/tv	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/graphy	0%	URL Reputation	safe	
http://https://143.244.140.214:808/	0%	URL Reputation	safe	
http://https://143.244.140.214:808/l?	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/N	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/	0%	URL Reputation	safe	
http://https://45.77.0.96:6891/derF	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/X	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/.0.96:6891/m	0%	Avira URL Cloud	safe	
http://https://185.56.219.47:8116/0	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/k	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/der6	0%	Avira URL Cloud	safe	
http://https://192.46.210.220/e	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/6	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/der.	0%	Avira URL Cloud	safe	
http://https://45.77.0.96:6891/Microsoft	0%	URL Reputation	safe	
http://https://14.77.0.96:6891/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://192.46.210.220/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.77.0.96	unknown	United States		20473	AS-CHOOPAUS	true
185.56.219.47	unknown	Italy		202675	KELIWEBIT	true
192.46.210.220	unknown	United States		5501	FRAUNHOFER-CLUSTER-BWResearchInstitutesspreadalloverGe	true
143.244.140.214	unknown	United States		174	COGENT-174US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510689
Start date:	28.10.2021
Start time:	05:09:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.980776.8232.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.bank.troj.evad.winDLL@11/1@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.5% (good quality ratio 14.5%) • Quality average: 78.9% • Quality standard deviation: 16%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:11:10	API Interceptor	25x Sleep call for process: rundll32.exe modified
05:11:13	API Interceptor	36x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.77.0.96	SecuriteInfo.com.Variant.Razy.980776.19527.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.5008.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	
185.56.219.47	SecuriteInfo.com.Variant.Razy.980776.19527.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.5008.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KELIWEBIT	SecuriteInfo.com.Variant.Razy.980776.19527.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.5008.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	• 185.56.219.47

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 185.56.219.47
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 185.56.219.47
AS-CHOOPAUS	SecuriteInfo.com.Variant.Razy.980776.19527.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.5008.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 45.77.0.96
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 45.77.0.96

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	SecuriteInfo.com.Variant.Razy.980776.19527.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.5008.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.19803.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.31954.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.10558.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.8232.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.30568.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.9478.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.28061.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.25006.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.28328.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.4470.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.14159.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.20807.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.27063.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.2260.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.12452.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.6851.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.2379.dll	Get hash	malicious	Browse	• 192.46.210.220
	SecuriteInfo.com.Variant.Razy.980776.10617.dll	Get hash	malicious	Browse	• 192.46.210.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.4145988351536807
Encrypted:	false
SSDEEP:	6:kKP148EMl/s8gFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:XqW/Y2kPlE99SNxAhUefit
MD5:	C824601B37315775244B5F3E184E9784
SHA1:	BE13B9570195223FB1905895CA1B5F9056176976
SHA-256:	F1E30158F2A271948414554A5A7EAB87E175607772C6850C875084DDDBF130BF
SHA-512:	BA4E3BD1F6697124F2706659144894B7CB9DF7CF66B8DED8BDDE4A59EE453FF21DAB20A1751B90A800A011EB4C74C8E9CFC412ACA17585E3091789A3595253C6
Malicious:	false
Reputation:	low
Preview:	p..... .....+9....(.....5..... .....^.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.439735798494042
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Variant.Razy.980776.8232.dll
File size:	1375232
MD5:	6df0687582c592e9860683a68858e082
SHA1:	53780def0699c055381746ce4ecebef8f17fd12d
SHA256:	90877ec621cc53fc31e693362e3b335a429aecc77abdbfd8b7d5d7493478f36d
SHA512:	43c27e2af87306bd6389af980e50dffc2b219868881db1a026d56eef7b012f94d11426cf82338901c7e950b463e1e7a8e8f0f7563040a3b5c013b4a39906a376
SSDEEP:	24576:anxqsL+DvNdnhMr5Lo6dOGcuQNrSH9d6N9eYWtZgDxxxSPnsqz7puATt5csRbu7i:acfk82uAJTI7EPswKwuG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..~...~...~.....8.z...w.X._...,...z...,...l...,...c...,...[.....<.f...~.....,.....,.....,3....,.....Rich~.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x4336b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT

General

Time Stamp:	0x5BBD73BC [Wed Oct 10 03:36:28 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	ccbe70d6d0d02f6248ca160d6a0bb85b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc5e2f	0xc6000	False	0.442065922901	data	6.47813133498	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc7000	0x80aec	0x80c00	False	0.534103837985	data	5.52051601648	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x148000	0x13ba0	0x1800	False	0.1875	DOS executable (block device driverpyright)	3.99635070896	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x15c000	0x72b4	0x7400	False	0.710264008621	data	6.69742088731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 192.46.210.220

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:09 UTC	0	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:09 UTC	0	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:10 UTC	4	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:10 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:12 UTC	4	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:12 UTC	5	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:12 UTC	9	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:12 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49786	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:51 UTC	49	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:51 UTC	49	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:51 UTC	54	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:51 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49787	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:52 UTC	54	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:52 UTC	54	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:53 UTC	59	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:52 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49799	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:58 UTC	59	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:58 UTC	59	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:59 UTC	64	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:59 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49800	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:59 UTC	64	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:59 UTC	64	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:12:00 UTC	69	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:12:00 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49806	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:12:08 UTC	69	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:12:08 UTC	69	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:12:09 UTC	73	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:12:09 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49810	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:12:16 UTC	74	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:12:16 UTC	74	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:12:17 UTC	78	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:12:16 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49823	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:12:24 UTC	79	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:12:24 UTC	79	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:12:25 UTC	83	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:12:24 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49752	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:20 UTC	9	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:20 UTC	9	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:21 UTC	14	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:21 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49753	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:21 UTC	14	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:21 UTC	14	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:22 UTC	19	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:22 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49760	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:28 UTC	19	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:28 UTC	19	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:28 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:28 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49761	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:28 UTC	24	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:28 UTC	24	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:29 UTC	29	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:29 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49768	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:36 UTC	29	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:36 UTC	29	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:37 UTC	34	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:36 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49769	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:37 UTC	34	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:37 UTC	34	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:37 UTC	39	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:37 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49776	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:43 UTC	39	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4814 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:43 UTC	39	OUT	Data Raw: e9 14 ae 38 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 37 cd bb 8c 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: 8#QZK?)D5=>\F[{!@}<60k7Sg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:44 UTC	44	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:44 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49779	192.46.210.220	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 03:11:44 UTC	44	OUT	POST / HTTP/1.1 Host: 192.46.210.220 Content-Length: 4802 Connection: Close Cache-Control: no-cache
2021-10-28 03:11:44 UTC	44	OUT	Data Raw: 0b 5c 98 14 10 0f 23 a1 51 b5 5a a3 4b 3f 1d 93 e5 fb 29 ab ad ff f2 44 04 13 80 c9 dd 06 c4 1c a4 a4 bd 35 3d 0f 83 b2 94 ac fd b9 85 18 c8 dd fe e0 7f 3e 9f 5c 1f 46 5b 7b 88 07 21 40 7d fd 3c fb 93 03 10 fc 36 95 01 ba 8b 30 6b 05 56 d3 bb ce 00 53 ff 67 eb 60 f6 41 72 31 97 d0 5d 17 8c 3e 91 70 4c 32 4c 65 54 c8 63 97 5d 23 fa 2a 14 6f de d4 1a 49 98 d0 cd f3 0d a7 96 2b ec 24 e9 2e 8f 05 fc 7b 03 b4 c5 35 3a b3 94 49 02 cb 9a 68 0a cf 6b b4 a2 ec e5 70 19 be 24 33 21 16 fe 6a 9c 5f a5 01 08 3e 5a 82 64 5c 75 b1 cc 6f fd 37 0c 85 1b b4 e9 c8 37 cc f0 0a a2 70 be f7 bb c5 89 e5 e1 46 d0 8d d5 1e 0a 93 8c 69 b6 41 f8 08 31 ff 6d d6 53 23 ed 8f cb 18 51 e2 66 24 5a 3a 93 1b 60 5d a3 3e 82 87 68 64 fe 36 9c a8 38 b1 94 8e fc 27 01 89 00 f2 78 71 a6 14 7a Data Ascii: \#QZK?)D5=>\F[{!@}<60kVSg`Ar1]>pL2LeTc]#*oI+$.{5:Ihkp$3!j_>Zd\uo77pFiA1mS#Qf$Z:`]>hd68'xqz
2021-10-28 03:11:45 UTC	49	IN	HTTP/1.1 403 Forbidden Server: nginx/1.15.12 Date: Thu, 28 Oct 2021 03:11:45 GMT Content-Type: text/plain; charset=utf-8 Connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4248 Parent PID: 4664

General

Start time:	05:10:01
Start date:	28/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll'
Imagebase:	0x1370000

File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.690396403.000000006E9F1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000003.431718268.00000000009E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 2248 Parent PID: 4248

General

Start time:	05:10:02
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll',#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5016 Parent PID: 4248

General

Start time:	05:10:02
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll,Bluewing
Imagebase:	0x380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000003.396279024.0000000004910000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6340 Parent PID: 2248

General

Start time:	05:10:02
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll',#1
Imagebase:	0x380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000003.404224619.0000000004740000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.690890687.000000006E9F1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: rundll32.exe PID: 6332 Parent PID: 4248

General

Start time:	05:10:07
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll,Earth
Imagebase:	0x380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000003.420461174.0000000004120000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6352 Parent PID: 4248

General

Start time:	05:10:11
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.980776.8232.dll,Masterjust
Imagebase:	0x380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000005.00000003.429863191.0000000003410000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis